Zeitschrift: Bulletin des Schweizerischen Elektrotechnischen Vereins, des Verbandes Schweizerischer Elektrizitätsunternehmen = Bulletin de l'Association suisse des électriciens, de l'Association des entreprises électriques suisses

Herausgeber: Schweizerischer Elektrotechnischer Verein ; Verband Schweizerischer Elektrizitätsunternehmen

Band: 86 (1995)

Heft: 19

Artikel: Leistungs- und Zuverlässigkeitsanalyse störungstoleranter Systeme : Grundlagen eines neuen Konzepts und beispielhafte Anwendung auf ein einfaches Computernetzwerk

Autor: Brenner, Andreas

DOI: https://doi.org/10.5169/seals-902485

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 02.07.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

Störungstolerante Systeme sind so konzipiert, dass sie bei Komponenten- oder Subsystemausfällen ihre geforderte Funktion fortführen können. Die Verwendung von solchen Systemen in verschiedenen technischen Anwendungsgebieten (Computertechnologie, Telekommunikation, Energieübertragung usw.) erfordert Analysemethoden, welche die Modellierung dieser Systeme erlauben. Weil sich bei störungstoleranten Systemen die abgegebene Leistung typischerweise in Abhängigkeit von auftretenden Ausfällen und durchgeführten Reparaturen ändert, muss eine adäquate Analyse die Wechselwirkung zwischen Leistungs- und Zuverlässigkeitsverhalten berücksichtigen. In diesem Artikel wird eine Methode vorgestellt, welche die kombinierte Leistungs-/Zuverlässigkeitsanalyse von reparierbaren, störungstoleranten Systemen ermöglicht.

Leistungs- und Zuverlässigkeitsanalyse störungstoleranter Systeme

Grundlagen eines neuen Konzepts und beispielhafte Anwendung auf ein einfaches Computernetzwerk

■ Andreas Brenner

Die zunehmenden Anforderungen an technische Systeme bezüglich Leistungs- und Zuverlässigkeitsverhalten erfordern einen hohen Grad an Störungstoleranz. Störungstolerante Systeme besitzen die Eigenschaft, dass sie ihre Funktion selbst beim Ausfall von Komponenten oder Subsystemen fortführen können. Bei einem oder mehreren Teilausfällen ist es jedoch wahrscheinlich, dass die zur Verfügung gestellte Leistung des Systems beeinträchtigt wird. Das Leistungsverhalten eines störungstoleranten Systems ändert sich deshalb typischerweise in Abhängigkeit von auftretenden Ausfällen und durchgeführten Reparaturen. Als Beispiel eines störungstoleranten Systems sei ein Multiprozessor-System erwähnt, wo anstelle eines einzelnen Prozessors mehrere Prozessoren parallel eingesetzt werden. Das System funktioniert, solange eine minimale Anzahl Prozessoren einwandfrei arbeiten. Der Ausfall einzelner Prozessoren beeinträchtigt jedoch direkt die vom System zur Verfügung gestellte Rechenleistung. Weitere Beispiele von störungstoleranten Systemen sind Telekommunikationsnetze, welche durch Mehrweg-Routing Fehlertoleranz-Eigenschaften aufweisen, oder elektrische Energieübertragungsnetze, bei welchen Störungstoleranz insbesondere aus Sicherheitsgründen gefordert wird.

Die traditionelle Zuverlässigkeitsanalyse beinhaltet hauptsächlich die Untersuchung des Systemverhaltens bezüglich den Aspekten *Zuverlässigkeit* und *Verfügbarkeit*. Die klassische Leistungsanalyse anderseits umfasst die Systembeurteilung bezüglich der abgegebenen *Leistung*, wobei davon ausgegangen wird, dass das System keine Ausfälle aufweist. Beide Konzepte der Systemanalyse wurden in der Vergangenheit getrennt angewendet. Die getrennte Systemanalyse bezüglich Leistungs- und Zuverlässigkeitsaspekten ist

Adresse des Autors:
Andreas Brenner, Dipl. El.-Ing. ETH, lic. oec. HSG, Professur für Zuverlässigkeitstechnik, Eidgenössische Technische Hochschule Zürich (ETH), Gloriastrasse 35, 8092 Zürich.

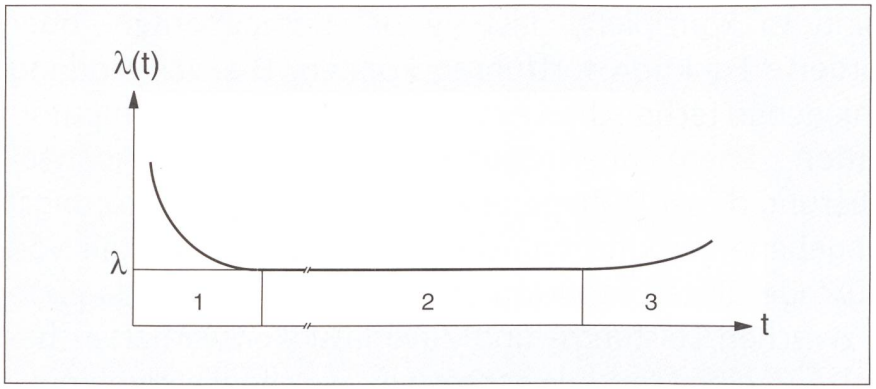

Bild 1 Typischer Verlauf der Ausfallrate $\lambda(t)$ einer Betrachtungseinheit in technischen Systemen

1 Phase der Frühausfälle
2 Phase der Ausfälle mit konstanter Ausfallrate
3 Phase der Verschleissausfälle

jedoch nur adäquat, wenn einzelne Komponenten- oder Subsystemausfälle die abgegebene Leistung des Systems nicht massgebend beeinflussen. Im folgenden wird ein Konzept vorgestellt, welches die kombinierte Leistungs- und Zuverlässigkeitsanalyse von störungstoleranten Systemen ermöglicht.

Wie misst man Zuverlässigkeit und Verfügbarkeit?

Definitionen und grundlegende Beziehungen

Die *Zuverlässigkeit* (Reliability) eines Systems ist ein Mass für die Eigenschaft, funktionstüchtig zu bleiben. Sie wird durch die Wahrscheinlichkeit angegeben, dass die *geforderte Funktion* unter *vorgegebenen Arbeitsbedingungen* während einer *festgelegten Zeitdauer* ausgeführt wird. Ein Ausfall tritt ein, wenn das System aufhört, die geforderte Funktion auszuführen. Bei Zuverlässigkeitsanalysen wird grundsätzlich zwischen einer geschätzten und einer vorausgesagten Zuverlässigkeit unterschieden. Während die geschätzte Zuverlässigkeit anhand von Prüfungen und statistischen Auswertungen ermittelt wird, erfolgt die Ermittlung der vorausgesagten Zuverlässigkeit analytisch anhand der Struktur des Systems.

In der Zuverlässigkeitsanalyse hat die Ausfallrate eine fundamentale Bedeutung. Die Ausfallrate ist die auf δt bezogene Wahrscheinlichkeit $\Pr\{t<\tau\leq t+\delta t \mid \tau>t\}$, dass eine Betrachtungseinheit (System, Komponente, Bauteil usw.) im Zeitintervall $(t, t+\delta t]$ ausfallen wird (d.h. $t<\tau\leq t+\delta t$), unter der Bedingung, dass sie zur Zeit $t=0$ neuwertig ist und im Zeitintervall $(0, t]$ nicht ausgefallen ist (d.h. $\tau>t$). Dabei bedeutet τ die ausfallfreie Arbeitszeit der Betrachtungseinheit. Für die Ausfallrate $\lambda(t)$ gilt

$$\lambda(t) = \lim_{\delta t \to 0} \frac{1}{\delta t} \Pr\{t < \tau \leq t + \delta t \mid \tau > t\} = -\frac{dR(t)/dt}{R(t)} \qquad (1)$$

wobei $R(t) = \Pr\{\tau > t\}$ die Zuverlässigkeitsfunktion der Betrachtungseinheit bezeichnet. Mit der Anfangsbedingung $R(0)=1$ folgt dann für die Zuverlässigkeitsfunktion $R(t) = \exp\left(-\int_0^t \lambda(x)\,dx\right)$. Falls die Ausfallrate konstant (zeitunabhängig) ist, das heisst für $\lambda(t) = \lambda$, gilt $R(t) = e^{-\lambda t}$.

Zuverlässigkeit realer Systeme

Der typische Verlauf der Ausfallrate $\lambda(t)$ realer Systeme (beispielsweise elektronischer Komponenten) ist in Bild 1 gezeigt. Eine erste Phase (1) kennzeichnet *Frühausfälle*, wobei sich die Ausfallrate im allgemeinen relativ schnell einer Phase mit einem konstanten Wert λ annähert. In dieser zweiten Phase der Ausfälle mit *konstanter Ausfallrate* (2) treten Ausfälle meistens plötzlich und rein zufällig auf. Mit zunehmender Betriebsdauer werden die Ausfälle wieder häufiger. Diese dritte Phase der *Verschleissausfälle* (3) ist auf Alterung und Abnützung der Betrachtungseinheit zurückzuführen.

Der Erwartungswert der ausfallfreien Arbeitszeit τ wird als *Mean Time to Failure (MTTF)* bezeichnet und kann wie folgt berechnet werden:

$$MTTF = E[\tau] = \int_0^\infty R(t)dt \qquad (2)$$

Für reparierbare Systeme ist es sinnvoll, neben der Zuverlässigkeitsfunktion zusätzlich die *Verfügbarkeit* (Availability) des Systems anzugeben. Die Verfügbarkeit eines Systems ist ein Mass für die Eigenschaft, zu einem gegebenen Zeitpunkt funktionstüchtig zu sein. Eine wichtige Form ist die *Punkt-Verfügbarkeit*, welche die Wahrscheinlichkeit angibt, dass das System zu einem bestimmten Zeitpunkt die geforderte Funktion unter vorgegebenen Arbeitsbedingungen ausführt. Für die Berechnung wird oft angenommen, dass das System kontinuierlich in Betrieb ist (Stillstand nur bei Systemausfall), dass alle Komponenten oder Subsysteme nach jeder Reparatur neuwertig sind und dass der Einfluss von menschlichen und logistischen Faktoren vernachlässigbar ist.

Modellierung von störungstoleranten Systemen

Beschreibung von Systemänderungen mit stochastischen Prozessen

Die Zuverlässigkeitsanalyse von reparierbaren, störungstoleranten Systemen erfolgt mit Hilfe stochastischer Prozesse [1]. Der zur Modellierung eines Systems verwendete stochastische Prozess beschreibt das Ausfall-/Reparaturverhalten dieses Systems und wird als *Strukturprozess* bezeichnet. Jede Kombination von funktionstüchtigen und ausgefallenen Komponenten oder Subsystemen ergibt einen (Struktur-)Zustand des Gesamtsystems. Die Gesamtheit aller Zustände bildet den Zustandsraum des stochastischen Prozesses. Übergänge zwischen Zuständen repräsentieren Änderungen des Systems, wie zum Beispiel den Ausfall einer Komponente oder umgekehrt ihre Reparatur. Für die Modellierung realer Systeme werden meistens zeitkontinuierliche stochastische Prozesse mit endlich vielen Zuständen verwendet. Bei einem zeitkontinuierlichen Prozess können Zustandsänderungen zu einem beliebigen Zeitpunkt stattfinden. Häufig wird dabei die Annahme getroffen, dass die zukünftige Entwicklung des Prozesses nur noch vom gegenwärtigen Zustand abhängt. Der Strukturprozess ist dann ein sogenannter *Markoff-Prozess* [1]. Insbesondere Systeme, welche konstante Ausfall- und Reparaturraten aufweisen, können mit Hilfe von solchen Markoff-Prozessen beschrieben werden.

Zur kombinierten Leistungs-/Zuverlässigkeitsanalyse von Systemen wird dem Strukturprozess zusätzlich eine *Leistungsstruktur* überlagert. Dabei werden für alle Zustände des Strukturprozesses Leistungsniveaus ermittelt. Diese beschreiben die Leistung des Systems, wenn es in einem bestimmten Zustand ist, wobei angenommen wird, dass das Leistungsniveau jeweils nur von diesem Zustand abhängt. Typische Leistungsbetrachtungen beziehen sich beispielsweise auf die verfügbare Bandbreite in einem Telekommunikationsnetz oder auf die Rechenleistung eines Computersystems. Der Strukturprozess bildet zusammen mit der Leistungsstruktur eine formale

Beschreibungstechnik, welche als *Stochastic Reward Model* (SRM) [2, 3] bezeichnet wird und die kombinierte Leistungs-/Zuverlässigkeitsanalyse von reparierbaren, störungstoleranten Systemen ermöglicht. Abhängig von den Verteilungsfunktionen der ausfallfreien Arbeits- und Reparaturzeiten einzelner Komponenten oder Subsysteme führt das SRM zu einem Markoff-, einem Semi-Markoff-, einem Markoff-regenerativen Prozess (auch semiregenerativer Prozess genannt) oder aber zu einem nicht-regenerativen Prozess mit überlagerter Leistungsstruktur. Die folgenden Betrachtungen beschränken sich auf den mathematisch einfachsten und meistverwendeten Typ, den Markoff-Prozess mit überlagerter Leistungsstruktur.

Markoff-Prozesse mit überlagerter Leistungsstruktur

Das Leistungs-/Zuverlässigkeitsverhalten eines reparierbaren, störungstoleranten Systems kann mit Hilfe eines Markoff-Prozesses mit überlagerter Leistungsstruktur (*Markov Reward Model*) [6, 7] beschrieben werden, falls alle Komponenten und Subsysteme (zeitlich) konstante Ausfall- und Reparaturraten aufweisen. Formal lässt sich der Markoff-Prozess mit überlagerter Leistungsstruktur wie folgt beschreiben: Der Zustandsraum dieses zeitkontinuierlichen Markoff-Prozesses $\{Z(t), t \geq 0\}$ ist mit Ω bezeichnet. Er kann in zwei komplementäre Teilmengen unterteilt werden: die Menge der Zustände, wo das System funktionstüchtig ist, U, und die Menge der Zustände, welche Systemausfälle repräsentieren, $\bar{U}$. Die Anzahl Zustände der Menge U ist mit $|U|$ bezeichnet. Zustände werden normalerweise mittels nichtnegativer Zahlen durchnumeriert (i), wobei ohne Einschränkung die ersten $|U|$ Zustände das funktionstüchtige System beschreiben. Die Leistungsstruktur ist durch den Zeilenvektor $\underline{r}$ gegeben, wobei jede Komponente r_i ($i \in \Omega$) das Leistungsniveau im Zustand i reflektiert. Wenn der Prozess im Zustand i eine Zeitdauer Δt verweilt, beträgt die kumulative Leistung $r_i \cdot \Delta t$.

Der Zeilenvektor $\underline{P}(t)$ mit Anfangsbedingung $\underline{P}(0)$ beschreibt das transiente Systemverhalten, wobei jede Komponente $P_i(t)$ ($i \in \Omega$) die Wahrscheinlichkeit angibt, dass das System zum Zeitpunkt t im Zustand i ist. Zur Bestimmung der Zuverlässigkeitsfunktion ist der erste Übergang von einem funktionstüchtigen zu einem ausgefallenen Zustand relevant. Angenommen, dass das System zur Zeit $t=0$ funktionstüchtig ist, beschreibt der Zeilenvektor $\underline{P}^{(u)}(t)$ mit Anfangsbedingung $\underline{P}^{(u)}(0)$ das ausfallfreie Verhalten des Systems, wobei die Komponente $P_i^{(u)}(t)$ ($i \in U$) die Wahrscheinlichkeit angibt, dass das System zur Zeit t im Zustand i ist, wenn kein Systemausfall im Intervall $(0, t]$ auftritt. Der Markoff-Prozess ist durch die Matrix der Übergangswahrscheinlichkeiten $\boldsymbol{Q} = [q_{ij}]$ charakterisiert. Die Elemente q_{ij} ($i,j \in \Omega$) dieser Matrix bezeichnen für $i \neq j$ die Übergangswahrscheinlichkeit vom Zustand i zum Zustand j. Die Diagonalelemente von $\boldsymbol{Q}$ sind durch $q_{ii} = -\Sigma_{j \neq i} q_{ij}$ gegeben. Der transiente Zustandsvektor $\underline{P}(t)$ kann mit Hilfe der folgenden Kolmogoroff-Differentialgleichung und gegebener Anfangsbedingung $\underline{P}(0)$ bestimmt werden:

$$\frac{d\underline{P}(t)}{dt} = \underline{P}(t)\,\boldsymbol{Q} \tag{3}$$

Der Wahrscheinlichkeitsvektor für ausfallfreies Verhalten $\underline{P}^{(u)}(t)$ mit Anfangsbedingung $\underline{P}^{(u)}(0)$ kann ebenfalls mit Hilfe von Gleichung (3) durch Verwendung der Untermatrix $\boldsymbol{Q}^{(u)} = [q_{ij}]$ der Grösse $|U| \cdot |U|$ mit Einträgen q_{ij} ($i,j \in U$) von $\boldsymbol{Q}$ bestimmt werden.

Systeme im stationären Zustand

Im Fall von reparierbaren Systemen kann der Zustand stationär werden, das heisst es existieren Lösungen für $d\underline{P}(t)/dt = 0$. Der entsprechende Zeilenvektor $\underline{\pi}$ wird *stationärer Zustandsvektor* genannt. Jede seiner Komponenten π_i ($i \in \Omega$) gibt die Wahrscheinlichkeit an, dass sich das System im stationären Verhalten im Zustand i befindet. Die Bestimmung des stationären Zustandsvektors $\underline{\pi}$ kann, entsprechend Gleichung (3), durch Auflösung des linearen Gleichungssystems $0 = \underline{\pi}\,\boldsymbol{Q}$ mit $\Sigma_{k \in \Omega} \pi_k = 1$ erfolgen.

Kombinierte Messgrössen für Leistung und Zuverlässigkeit

Eine wichtige kombinierte Messgrösse für störungstolerante Systeme ist die *Leistungs-Zuverlässigkeit*, $PR(t)$ (Performance Reliability). Sie gibt die momentane Leistung zum Zeitpunkt t an, wenn im Intervall $(0, t]$ kein Systemausfall eintritt. Sie beschreibt das Leistungsverhalten des Systems während der ausfallfreien Arbeitszeit und kann wie folgt berechnet werden

$$PR(t) = \sum_{k \in U} r_k P_k^{(u)}(t) \tag{4}$$

Ein weiteres wichtiges Mass ist die *erwartete kumulative Systemleistung vor dem ersten Systemausfall*, *MPTF* (Mean Performance to Failure). Sie ist gegeben durch

$$MPTF = \sum_{k \in U} r_k \int_0^\infty P_k^{(u)}(x)dx = \int_0^\infty PR(x)dx \tag{5}$$

Für die erwartete *momentane Systemleistung* zum Zeitpunkt t, als Leistungs-Verfügbarkeit $PA(t)$ (Performance Availability) bezeichnet, folgt

$$PA(t) = \sum_{k \in \Omega} r_k P_k(t) \tag{6}$$

Die *stationäre Leistungs-Verfügbarkeit* gibt die erwartete Leistung im stationären Systemverhalten an und ist durch $PA_S = \Sigma_{k \in \Omega} r_k \pi_k$ gegeben. Die *durchschnittliche Leistungs-Verfügbarkeit* während des Zeitintervalls $(0, t]$ ist $APA(t) = (1/t)\int_0^t PA(x)dx$.

Von grosser Bedeutung für die Bewertung des Leistungs- und Zuverlässigkeitsverhaltens eines Systems ist schliesslich die *erwartete kumulative Leistung*, $CP(t)$ (Cumulative Performance). Sie lässt sich folgendermassen berechnen

$$CP(t) = \sum_{k \in \Omega} r_k \int_0^t P_k(x)dx \tag{7}$$

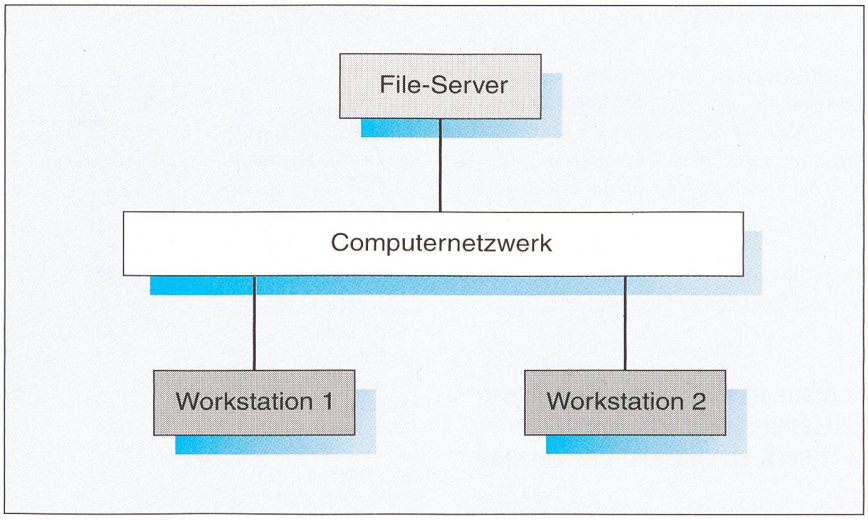

Bild 2 Konfiguration eines einfachen, störungstoleranten Computersystems
Das System wird als funktionstüchtig betrachtet, solange mindestens eine Workstation, das Computernetzwerk und der File-Server funktionieren.

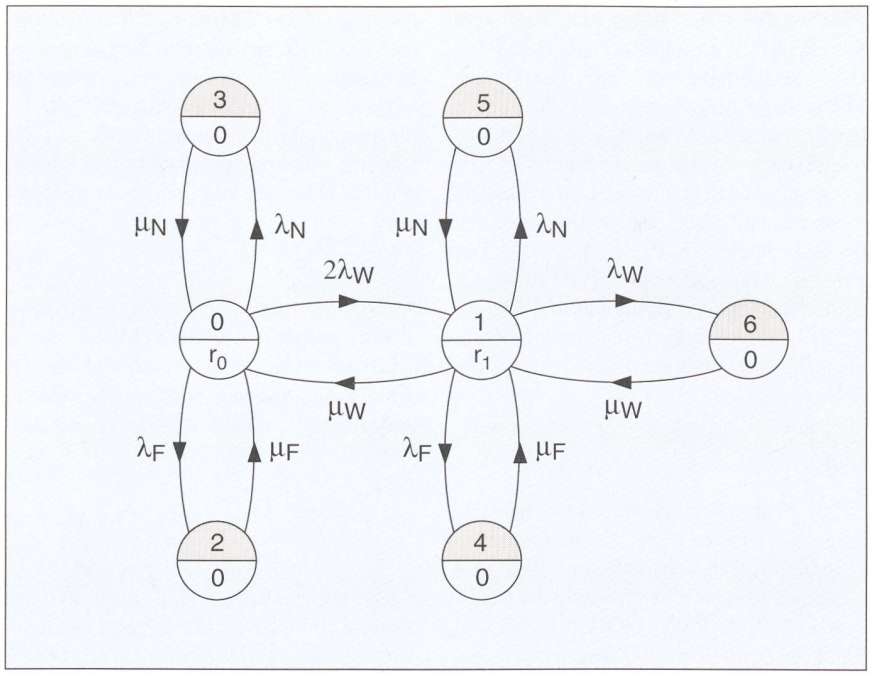

Bild 3 Diagramm eines Markoff-Prozesses mit überlagerter Leistungsstruktur

Das Diagramm charakterisiert die Zustände und die Zustandsänderungen des in Bild 2 dargestellten Computersystems. Zustände, welche Systemausfälle repräsentieren, sind schattiert dargestellt.

λ_W, λ_N, λ_F	Ausfallrate einer Workstation, des Computernetzwerks und des File-Servers
μ_W, μ_N und μ_F	Reparaturrate einer Workstation, des Computernetzwerks und des File-Servers
r_0, r_1	Leistungsniveaus der funktionsfähigen Zustände 0 und 1

Verteilungsfunktionen der momentanen und kumulativen Leistung können in ähnlicher Weise berechnet werden [2, 6].

Spezialfall einer binären Leistungsstruktur

Wird als Spezialfall anstelle einer allgemeinen nur eine *binäre* Leistungsstruktur verwendet, bei der die Leistungsniveaus von funktionstüchtigen Zuständen 1 und für Ausfallzustände 0 betragen, erhält man wieder direkt die bekannten klassischen Zuverlässigkeitskenngrössen. Die Leistungs-Zuverlässigkeit führt zur klassischen Zuverlässigkeitsfunktion, und aus der erwarteten kumulativen Systemleistung vor dem ersten Systemausfall (*MPTF*) folgt die erwartete ausfallfreie Arbeitszeit (*MTTF*). Aus der Leistungs-Verfügbarkeit resultiert die Punkt-Verfügbarkeit, und aus der erwarteten kumulativen Leistung schliesslich folgt die kumulative ausfallfreie Arbeitszeit während des Zeitintervalls $(0, t]$.

Kombinierte Leistungs-/Zuverlässigkeitsanalyse für ein Computernetzwerk als illustratives Beispiel

Die kombinierte Leistungs-/Zuverlässigkeitsanalyse wird im folgenden mit Hilfe eines praktischen Beispiels näher erläutert. Wir betrachten ein Computersystem, bestehend aus zwei identischen Workstations, welche, wie in Bild 2 gezeigt, via ein Computernetzwerk mit einem File-Server verbunden sind.

Das System wird als funktionstüchtig betrachtet, solange mindestens eine Workstation, das Computernetzwerk und der File-Server funktionieren. Es wird angenommen, dass die Ausfall- und Reparaturraten der Subsysteme als zeitlich konstant angenommen werden können. Die Ausfallraten einer Workstation, des Computernetzwerks sowie des File-Servers sind mit λ_W, λ_N und λ_F bezeichnet, während die entsprechenden Reparaturraten mit μ_W, μ_N und μ_F bezeichnet sind. Weiter wird angenommen, dass eine Reparaturmannschaft zur Verfügung steht. Das Computernetzwerk und der File-Server haben bei der Reparatur höhere Priorität gegenüber den Workstations. Für die Modellierung wird ebenfalls angenommen, dass während der Reparatur eines Ausfalls auf Systemebene keine weiteren Ausfälle mehr auftreten.

Unter diesen Annahmen lässt sich das Leistungs-/Zuverlässigkeitsverhalten des Computersystems mit einem Markoff-Prozess mit überlagerter Leistungsstruktur modellieren. Bild 3 zeigt das Diagramm der Übergangswahrscheinlichkeiten, wobei für alle ausgefallenen Zustände ein Leistungsniveau von Null angenommen ist. Im Zustand 0 arbeitet das System mit zwei und im Zustand 1 mit einer Workstation. Das Leistungsverhalten ist in diesen Zuständen durch die Leistungsniveaus r_0 und r_1 beschrieben. Die Zustände 2 und 4 stellen einen Systemausfall dar, welcher durch den Ausfall des File-Servers verursacht wird. Der Systemausfall in den Zuständen 3 und 5 resultiert vom Computernetzwerk. Im Zustand 6 tritt der Systemausfall infolge Ausfalls der beiden Workstations auf.

Als Leistungsparameter r_i wird die Rechenkapazität des Computersystems betrachtet. Es wird angenommen, dass die Systemleistung proportional zur Anzahl der arbeitenden Workstations ist. Entsprechend sind die Leistungsniveaus der funktionstüchtigen Zustände durch $r_0 = 2\gamma$ und $r_1 = \gamma$ gegeben, wobei γ die Rechenkapazität einer Workstation bezeichnet. Alternativ könnte sich eine detailliertere Leistungsanalyse auf Job-Wartezeiten oder andere Parameter beziehen.

Unter der Annahme, dass zum Zeitnullpunkt alle Subsysteme funktionieren, ist die Zuverlässigkeitsfunktion $R_0(t)$ des

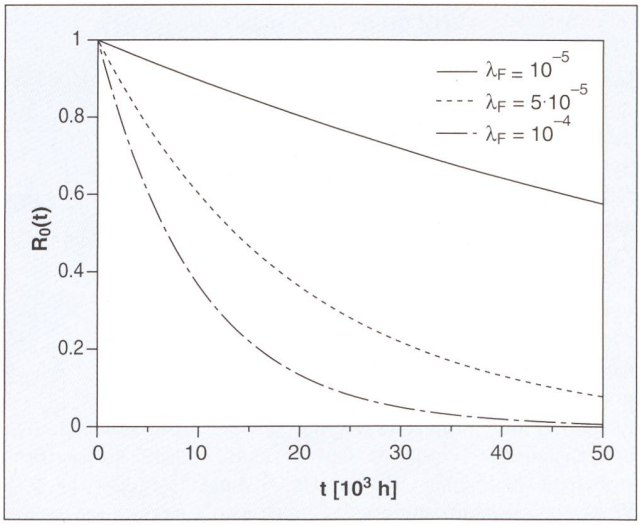

Bild 4 Berechnete Zuverlässigkeitsfunktion des Computersystems nach Bild 2

Die Zuverlässigkeitsfunktion $R_0(t)$ gibt die Wahrscheinlichkeit an, dass sich das System, welches sich zur Zeit $t = 0$ im Zustand 0 befindet, sich in der Zeit zwischen 0 und t ausnahmslos immer entweder im Zustand 0 oder 1 befindet.
Die für die Berechnung eingesetzten Ausfall- und Reparaturraten sowie die Leistungsniveaus sind im Text und jene für λ_F (in h^{-1}) im Bild angegeben.

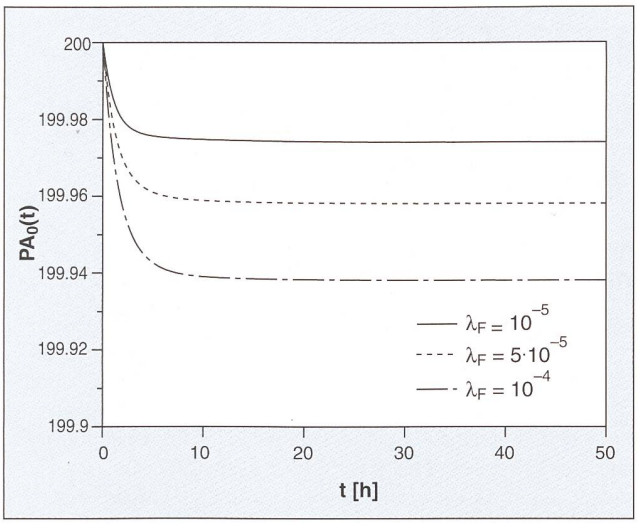

Bild 5 Berechnete Leistungs-Verfügbarkeit $PA_0(t)$ des Computersystems nach Bild 2

Numerische Annahmen und Anfangsbedingung: wie in Bild 4

Computersystems in Bild 4 für verschiedene Ausfallraten λ_F des File-Servers gezeigt. Für die Ausfallraten einer Workstation und des Computernetzwerks sind Werte von $\lambda_W = 10^{-4}$ h^{-1} und $\lambda_N = 10^{-6}$ h^{-1} angenommen, während die angenommenen Reparaturraten $\mu_W = 1$ h^{-1}, $\mu_F = 0{,}5$ h^{-1} und $\mu_N = 0{,}1$ h^{-1} betragen. Die mittlere ausfallfreie Arbeitszeit beträgt somit im Beispiel für eine Workstation $1/\lambda_W = 10^4$ h und die mittlere Reparaturzeit $1/\mu_W = 1$ h.

Die Zuverlässigkeitsfunktion $R_0(t)$ gibt die Wahrscheinlichkeit an, dass kein Systemausfall im Intervall $(0, t]$ auftreten wird. Aus Bild 4 ist ersichtlich, dass sich die Zuverlässigkeitscharakteristik des Computersystems stark verbessern lässt, falls die Ausfallrate des File-Servers verringert wird. Die Leistungs-Verfügbarkeit $PA_0(t)$ ist in Bild 5 für dieselben Werte der File-Server-Ausfallraten gezeigt, wobei ebenfalls angenommen ist, dass zum Zeitnullpunkt keine Subsysteme ausgefallen sind. Die Rechenkapazität γ einer Workstation beträgt 100 Jobs/Stunde. Die Leistungs-Verfügbarkeit gibt die erwartete Rechenkapazität des Computersystems zur Zeit t an. Man stellt fest, dass das stationäre Systemverhalten schon nach kurzer Zeit erreicht wird und die Sensitivität bezüglich der File-Server-Ausfallrate im Vergleich zur Zuverlässigkeit relativ gering ist.

In Tabelle I sind weitere Leistungs-/Zuverlässigkeitskenngrössen des Computersystems gezeigt: die erwartete kumulative Rechenkapazität vor dem ersten Systemausfall, $MPTF_0$, unter der Bedingung, dass zum Zeitnullpunkt alle Subsysteme arbeiten, die System-Unverfügbarkeit im stationären Systemverhalten, $(1-A_S)$, sowie die erwartete Zeit in Stunden, DT_S [1 Jahr], während der das System im stationären Verhalten in einem Zeitintervall von einem Jahr ausgefallen ist.

Approximationsmethoden reduzieren den Rechenaufwand

Die Leistungs-/Zuverlässigkeitsanalyse von komplexen Systemen führt zu Modellen, welche kaum ohne die Verwendung von Computerprogrammen gelöst werden können. Dies ist hauptsächlich auf den mit zunehmender Systemkomplexität verbundenen exponentiellen Anstieg der Anzahl Zustände zurückzuführen. Die Anzahl Zustände des Strukturprozesses kann für ein allgemeines System mit m Komponenten oder Subsystemen mehr als 2^m betragen. Falls der Strukturprozess M Zustände hat, muss für die Bestimmung von zeitabhängigen Leistungs-/Zuverlässigkeitsmessgrössen ein System von M Differentialgleichungen gelöst werden. Für die Ermittlung des stationären Systemverhaltens sowie der erwarteten ausfallfreien Arbeitszeit $MTTF$ oder der kumulativen Systemleistung vor dem ersten Systemausfall $MPTF$ gehen die M Differentialgleichungen in M lineare Gleichungen über [1, 3].

Zur Reduktion der Modellkomplexität können verschiedene Approximationsverfahren, wie beispielsweise die Zusammenlegung oder Vernachlässigung von Zuständen, angewendet werden [1, 5]. Bei der *Methode der Zustands-Zusammenlegung* zum Beispiel, werden Ereignisse, welche bezüglich Änderungen des Ausfall-/Reparatur- und Leistungsverhaltens ähnlich sind, zusammengefasst. Dadurch kann die Anzahl Zustände des Zustandsraumes beträchtlich reduziert werden. Bei der *Methode der Zustands-Vernachlässigung* anderseits, werden Zustände mit geringer Wahrscheinlichkeit identifiziert und vernachlässigt. Dabei entsteht ebenfalls ein neues Modell mit reduziertem Zustandsraum, wobei ein Approximationsfehler resultiert, welcher um so grösser ist, je mehr Zustände vernachlässigt werden. Eine weitere, systematische Näherungsmethode erhält man schliesslich, falls nur Zustände bis zu einer bestimmten Anzahl ausgefallener Komponenten oder Subsysteme berücksichtigt werden. Diese Methode ergibt insbesondere für hochzuverlässige Systeme, wie beispielsweise Telekommunikationsnetze, sehr gute Näherungen [4].

Schlussfolgerungen

Störungstolerante Systeme führen ihre geforderte Funktion selbst nach bestimmten Komponenten- oder Subsystemausfällen fort. Dabei ist es jedoch wahrscheinlich, dass die abgegebene Systemleistung beeinträchtigt wird. Bei der Modellierung von störungstoleranten Systemen muss deshalb der Effekt des Zuverlässigkeitsverhaltens auf die Leistungsabgabe berücksichtigt werden. Die hier vorgestellte Methode erlaubt neu eine kombinierte Leistungs-/Zuverlässigkeitsanalyse von reparierbaren, störungstoleranten Systemen, unter der Bedingung, dass die Ausfall- und Reparaturraten als konstant angenommen werden können. Die Bedeutung dieser Analyse ist entsprechend gross für Systeme, bei welchen eine geschätzte Leistungs-/Zuverlässigkeitsanalyse anhand einer statistischen Datenauswertung ent-

Leistungs-/Zuverlässigkeitsmass	File-Server-Ausfallrate		
	$\lambda_F = 10^{-4}$ h^{-1}	$\lambda_F = 5 \cdot 10^{-5}$ h^{-1}	$\lambda_F = 10^{-5}$ h^{-1}
$MPTF_0$	$1{,}979 \cdot 10^6$ Jobs	$3{,}920 \cdot 10^6$ Jobs	$1{,}815 \cdot 10^7$ Jobs
$1 - A_S$	$2{,}100 \cdot 10^{-4}$	$1{,}100 \cdot 10^{-4}$	$3{,}002 \cdot 10^{-5}$
DT_S[1 Jahr]	1,839 h	0,964 h	0,263 h

Tabelle I Leistungs-/Zuverlässigkeitskenngrössen des Computersystems für verschiedene File-Server-Ausfallraten

$MPTF_0$ Erwartete kumulative Systemleistung vor dem ersten Systemausfall
$1 - A_S$ System-Unverfügbarkeit im stationären Systemverhalten
DT_S[1 Jahr] Erwartete Zeit, während der das System im stationären Verhalten während eines Jahres ausgefallen ist

weder zu umständlich oder gar nicht möglich ist – zum Beispiel, weil das System noch nicht realisiert ist oder weil der Betrachtungszeitraum für aussagekräftige Resultate zu gross wird.

Literatur

[1] *A. Birolini:* Quality and Reliability of Technical Systems: Theory – Practice – Management. Springer, Berlin, 1994.

[2] *A. Bobbio:* Stochastic reward models in performance/reliability analysis. Journal on Communications XLIII (1) (1992), p. 27–35.

[3] *A. Brenner:* Stochastic reward models for performance and dependability analysis of fault-tolerant systems. Technical Report DS3, ETH Zurich, Reliability Laboratory 1995.

[4] *A. Brenner:* Performance and dependability analysis of fault-tolerant networks. Microelectronics and Reliability, to appear.

[5] *A. Brenner:* Numerical evaluation and approximations of stochastic reward models, Technical Report DS5, ETH Zurich, Reliability Laboratory 1995.

[6] *K. S. Trivedi, J. Muppala, S. Woolet* and *B. Haverkort:* Composite performance and dependability analysis. Performance Evaluation 14(3&4) (1992), p. 197–215.

[7] *K. S. Trivedi, B. Haverkort, A. Rindos* and *V. Mainkar:* Techniques and tools for reliability and performance evaluation: problems and perspectives. In: G. Haring and G. Kotsis, Eds., Computer Performance Evaluation: Modelling Techniques and Tools. 7th International Conference Vienna, Austria, May 1994. Springer, Berlin, 1994.

Analyse de performance et de fiabilité des systèmes tolérants à l'égard des défauts

Bases d'un nouveau concept et leur application à l'exemple d'un réseau d'ordinateurs simple

Les systèmes tolérants à l'égard des défauts sont construits de manière à pouvoir assumer la fonction exigée même en cas de défaillance de composants ou de sous-systèmes. L'utilisation de tels systèmes dans divers domaines techniques d'application (télécommunication, transport d'énergie, etc.) exige des méthodes d'analyse permettant la modélisation de ces systèmes. Etant donné que la performance fournie par les systèmes tolérants à l'égard des défauts varie normalement en fonction des défauts qui apparaissent et des réparations effectuées, une analyse séparée de la performance et de la fiabilité peut aboutir à des résultats imprécis et à des conclusions erronées. Le présent article décrit une méthode qui permet une analyse combinée de performance et de fiabilité des systèmes réparables tolérants à l'égard des défauts.

La méthode est expliquée dans le cas d'un système d'ordinateurs simple selon figure 2. Le système réparable est considéré comme étant à même de fonctionner tant qu'au moins une des stations de travail et le réseau ainsi que le serveur fonctionnent. Le système est caractérisé par le diagramme de la figure 3 et les taux de défauts qui y sont indiqués λ_W, λ_N et λ_F, les taux de réparation μ_W, μ_N et μ_F ainsi que les niveaux de performance r_0 et r_1 aux états 0 et 1. Les autres états 2–6 représentent des défaillances du système (performance de calcul zéro). Sur la base de ces hypothèses, il est possible de calculer la fonction de fiabilité $R_0(t)$ du système d'ordinateurs (fig. 4), la disponibilité de performance $PA_0(t)$ (fig. 5) ainsi que d'autres caractéristiques de performance/fiabilité du système d'ordinateurs (tab. I).

SEV/ASE

Kennen Sie die ITG?

Die Informationstechnische Gesellschaft des SEV (ITG) ist ein *nationales Forum* zur Behandlung aktueller Probleme im Bereich der Elektronik und Informationstechnik. Als *Fachgesellschaft des Schweizerischen Elektrotechnischen Vereins* (SEV) steht sie allen interessierten Fachleuten und Anwendern aus dem Gebiet der Informationstechnik offen.

Auskünfte und Unterlagen erhalten Sie beim Schweizerischen Elektrotechnischen Verein, Luppmenstrasse 1, 8320 Fehraltorf, Telefon 01 956 11 11.